Extra handout: Reducing polynomials modulo p

Steven Charlton, Algebra Tutorials 2015–2016
http://maths.dur.ac.uk/users/steven.charlton/algebra2_1516/

Recall the remark in Problems Class 2, Question 1 about reducing polynomials modulo a prime p.

Proposition. *Suppose $f(x) \in \mathbb{Z}[x]$ is a polynomial. Consider the reduction $\overline{f}(x)$ modulo p, and suppose $\deg(f) = \deg(\overline{f})$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, then $\overline{f}(x)$ is reducible in $\mathbb{Z}/p[x]$. Or by the contrapositive: if $\overline{f}(x)$ is irreducible in $\mathbb{Z}/p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

This gives another irreducibility test for polynomials. (Or as in the Problems Class, and in Tutorial 2, Question 3 the ideas can be used as a stepping-stone to deduce certain degree factors cannot occur.)

Example. Show each polynomial $f_{k,\ell}(x)$ in the following family is irreducible, where

$$f_{k,\ell}(x) = x^5 + (2k+1)x^2 + (2\ell+1)\,,$$

for integers $k, \ell \in \mathbb{Z}$.

We can't apply Eisenstein since we don't know what primes divide $2k+1$ and $2\ell+1$; no primes work for x^5+3x^2+1 where $k=1$ and $\ell=0$. Similarly we can't (easily) apply the rational root test and would have to check for quadratic factors anyway.

Reducing modulo 2 gives the polynomial $\overline{f}_{k,\ell}(x) = x^5 + x^2 + \overline{1}$ in $\mathbb{Z}/2[x]$. We can check easily it has no roots by substituting in $x = \overline{0}$, and $x = \overline{1}$. We still need to check if $\overline{f}_{k,\ell}(x)$ has a quadratic factor, but the only irreducible quadratic in $\mathbb{Z}/2[x]$ is $x^2 + x + 1$. (Why?) Then by polynomial long division, we can see that

$$x^5 + x^2 + \overline{1} = (x^2 + x + \overline{1})(x^3 + x^2) + (\overline{1}) \quad \text{in } \mathbb{Z}/2[x]\,,$$

so $\overline{f}_{k,\ell}(x)$ cannot have a quadratic factor. (Why is this sufficient?)

This shows that $\overline{f}_{k,\ell}(x)$ is irreducible in $\mathbb{Z}/2[x]$, and hence we deduce that $f_{k,\ell}(x) = x^5 + (2k+1)x^2 + (2\ell+1)$ is irreducible for every $k, \ell \in \mathbb{Z}$.

One might wonder if any irreducible polynomial can be detected in such a manner. Given an irreducible polynomial $f(x)$, can we always find a prime p for which $\overline{f}(x)$ is irreducible in $\mathbb{Z}/p[x]$? The answer is no! But there is some interesting maths behind the general phenomenon.

For the moment, let's consider the polynomial $f(x) = x^4 - 10x^2 + 1$.

Exercise. Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$. (Check for roots and quadratic factors.)

1 Behaviour modulo p

Let's look at how this $f(x)$ factors modulo p, for various primes.

Prime p	Factorisation of $f(x)$ modulo p
2	$(1+x)^4$
3	$(1+x^2)^2$
5	$(2+x^2)(3+x^2)$
7	$(6+x+x^2)(6+6x+x^2)$
11	$(1+x+x^2)(1+10x+x^2)$
13	$(1+5x+x^2)(1+8x+x^2)$
17	$(16+5x+x^2)(16+12x+x^2)$
19	$(4+x^2)(5+x^2)$
23	$(2+x)(11+x)(12+x)(21+x)$
29	$(8+x^2)(11+x^2)$
31	$(30+15x+x^2)(30+16x+x^2)$
37	$(1+7x+x^2)(1+30x+x^2)$
41	$(40+7x+x^2)(40+34x+x^2)$
43	$(9+x^2)(24+x^2)$
47	$(5+x)(19+x)(28+x)(42+x)$

Something curious indeed is happening here! Every factor modulo p seems to have the same degree – it never factors as linear $\times$ cubic, or linear^2 $\times$ quadratic. And it looks like $f(x)$ is always reducible modulo p.

2 Elementary explanation

We can give an elementary proof of this by making use of the following lemma.

Lemma. *If* 2 *and* 3 *are not squares modulo* p*, then* 6 *is a square modulo* p*.*

Proof. $((\mathbb{Z}/p)^*, \cdot)$ is a cyclic group of order $p-1$, generated say by g. Then $2 = g^{2k+1}$ and $3 = g^{2\ell+1}$, which means $6 = g^{2k+2\ell+2} = (g^{k+\ell+1})^2$. □

Now write

$$\begin{aligned} f(x) &= (x^2-1)^2 - 2(2x)^2 \\ &= (x^2+1)^2 - 3(2x)^2 \\ &= (x^2-5)^2 - 6(2)^2\,. \end{aligned}$$

Suppose 2 is a square modulo p, that is $\alpha^2 = \overline{2}$, for some $\alpha \in \mathbb{Z}/p$. Then modulo p the first expression factors as

$$(x^2-\overline{1})^2 - \overline{2}(\overline{2}x)^2 = (x^2-1)^2 - (\overline{2}\alpha x)^2$$

$$= (x^2 + \overline{2}\alpha x - \overline{1})(x^2 - \overline{2}\alpha x - \overline{1})\,. \tag{1}$$

If $\overline{3} = \beta^2$ modulo p, then the second expression factors modulo p as

$$(x^2 + \overline{1})^2 - \overline{3}(\overline{2}x)^2 = (x^2 + \overline{2}\beta x + \overline{1})(x^2 - \overline{2}\beta x + \overline{1})\,. \tag{2}$$

Otherwise 2 and 3 are not squares modulo p, and so by the lemma, 6 is a square. Write $\overline{6} = \gamma^2$. Then this time, the third expression factors modulo p as

$$(x^2 - \overline{5})^2 - \overline{6}(\overline{2})^2 = (x^2 - (\overline{5} - \overline{2}\gamma))(x^2 - (\overline{5} + \overline{2}\gamma))\,. \tag{3}$$

No matter what, $f(x)$ is the difference of two squares in $\mathbb{Z}/p[x]$ and so is always reducible modulo p.

Observe now that if one of the quadratic factors in Equation 1 or Equation 2 is reducible, then it has a root x_0, say. But $-x_0$ is a root of the other factor, which means it too is reducible. Either both quadratic factors are irreducible, or they reduce into 4 linear factors.

Now consider Equation 3. If one of the factors has a root, we can assume it is $x^2 - (\overline{5} - \overline{2}\gamma)$ by swapping $\gamma \leftrightarrow -\gamma$. Say the root is δ. Then δ is a root of $f(x)$ modulo p. Since $\overline{f}(\overline{0}) = \overline{1}$, δ is non-zero. And $\delta^2 - \overline{1} = \overline{4} - \overline{2}\gamma = \overline{2}(\overline{1} - \gamma)$. Use this when plugging δ into the expression for $\overline{f}(x)$ in Equation 1. We get

$$\overline{0} = (\delta^2 - \overline{1})^2 - \overline{2}(\overline{2}\delta)^2 = (\overline{2}(\overline{1} - \gamma))^2 - \overline{2}(\overline{2}\delta)^2\,.$$

Either $\overline{2} = \overline{0} = \overline{0}^2$. Or $\overline{2} \neq \overline{0}$, so $\overline{2}\delta \neq 0$ and we can write

$$\overline{2} = (\delta^2 - \overline{1})^2(\overline{2}\delta)^{-2}\,.$$

In both cases $\overline{2}$ is a square modulo p, and we conclude from the result above about Equation 1 that $f(x)$ must factor as 4 linear terms.

This shows that modulo p, the polynomial $f(x)$ factors always as linear^4 or quadratic^2. No other factorisation is possible.

3 Deeper explanation

The deeper reason why $f(x)$ exhibits the above factorisation behaviour modulo p has to do with *Galois Theory*, *Number Theory*, and the interplay between the two. Until you learn about Galois Theory and Number Theory, what's written below probably won't make much sense. So take Galois Theory and Number Theory next year to learn more.

The polynomial $f(x) = x^4 - 10x^2 + 1$ is the *minimal polynomial* for $\sqrt{2} + \sqrt{3}$. This means it is the smallest degree polynomial with has $\sqrt{2} + \sqrt{3}$ as a root.

Galois Theory can study the symmetries of the field extension $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ of $\mathbb{Q}$. It shows the group of symmetries is $\mathbb{Z}/2 \times \mathbb{Z}/2$, generated by $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$ and $\tau\colon \sqrt{3} \mapsto -\sqrt{3}$. When the number of symmetries equals the degree of the polynomial $f(x)$, the extension is called *Galois*. And the group of symmetries is called the *Galois group* of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$.

Number Theory can study how the prime number p (or rather the prime ideal (p)) factors in the *ring of integers* of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

A result of Dedekind relates the factorisation of (p) to the factorisation modulo p of the polynomial $f(x)$ which defines the field. The degrees of factors of $\overline{f}(x)$ correspond to the *inertial degrees* of the various prime ideals into which (p) factors.

Attached to each prime ideal in the factorisation of (p), there is a *decomposition group*. This group is cyclic, and can be viewed as a subgroup of the Galois group when the extension is Galois. The number of factors (p) splits into is given by the ratio of sizes of the Galois group and the decomposition group.

If the extension is Galois, acting with the Galois group shows that each prime ideal above (p) has the same inertial degree. But this means exactly that the factors of $f(x)$ modulo p all have the same degree!

If the Galois group is not cyclic, ratio of Galois group to decomposition group is $\neq 1$, so (p) must split into ≥ 2 factors. This means the polynomial $f(x)$ splits into ≥ 2 factors. Which means $f(x)$ modulo p is always reducible!

Example. 1) The polynomial $f(x) = x^6 + 108$ defines a Galois extension, which has Galois group S_3 (non-cyclic). This means the polynomial will always be reducible modulo p, and the factors will all have the same degree.

2) The polynomial $f(x) = x^4 + 29x^2 + 29$ defines a Galois extension, which has Galois group $\mathbb{Z}_4$ (cyclic). This means the polynomial might be irreducible modulo some primes (indeed this happens). But when it is reducible, the factors will always have the same degree.

3) The polynomial $f(x) = x^{12} - 16x^9 - 34x^6 + 28x^3 - 2$ does not define a Galois extension, but it does contain a Galois *subextension* which has Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$ (non-cyclic). This will force the polynomial to be reducible modulo all primes, but the factors might have different degrees (indeed this happens).

You might like to investigating the factorisations modulo p using `Maple`, or `Mathematica` or `WolframAlpha`.